Caribbean Journal of Philosophy, Vol. 6, No. 1, 2014 (Published July 2017)

CYBERETHICS, SPYWARE AND THE WAR ON TERRORISM IN AN AGE OF LIBERAL DEMOCRACY

by

Dr. Abosede Priscilla Ipadeola
Department of Philosophy
University of Ibadan
Ibadan, Nigeria

Abstract

This essay juxtaposes the notion of human freedom, which liberal democracy advocates, with the menace of terrorism, which is fast becoming an atrocious impediment to national development and social order in virtually all the countries of our global world. Since the commencement of the information revolution age, there is hardly anything that can be done in the world without recourse to Information and Communications Technology (ICT). Hence, in virtually every activity known to or undertaken by humans today, information technology, especially the internet plays a very significant role. Terrorist and counter-terrorist efforts also rely heavily on the ICT. Terrorists now mostly plan their attacks using one form of communication or information technology platform or the other. Hence, an effective measure against terrorist activities, especially in this era of information revolution, cannot afford not to look in the direction of the ICT in finding immediate and urgent solution to the problem of security threats which terrorism poses. A tool of surveillance which can be used to uncover terrorists' plans in order to forestall attacks or to bring terrorists to book after an attack has been perpetrated is spyware. However, the challenge, which the use of spyware by government security agencies poses is that it does not promote the human right to privacy and freedom. This paper argues that this quandary can be overcome with the adoption of utilitarianism, a traditional ethical theory. In this sense, what brings safety to the greatest number is considered ethical.

Key Words: Cyberethics, Liberal democracy, Utilitarianism, Electronic surveillance, Terrorism.

Introduction

With the ending of the Cold War, 'liberal democracy' seems to have become the only good form of government, with many countries around the world undergoing 'democratisation' (Chan 2002, 11). The belief in individualism involves seeking the maximum area of free choice and action compatible with an orderly society, and minimizing not only the governmental or social restraints on action, but also any *external intrusion on individual privacy* (Carter 2013, 118; my italics).

Information and communications technologies (ICT) have become more deeply intertwined with our daily activities in both social and professional spheres. As these technologies expand, both in utility and in availability, it stands to reason that terrorist groups have made commensurate advancements in leveraging modern ICTs for their goals and objectives (Espeseth et al 2013, 91).

Since terrorists struck at the World Trade Centre in the United States of America in September 2001, the menace of terrorism has become an issue of global concern. Terrorist attacks have since spread to many other countries, which erstwhile were considered peaceful. Also, apart from the Al-Qaeda, which was directly linked to the 'September 11' attack, several other groups have sprung up in many other countries. For example, the Taliban in Afghanistan, the Al-Shabaab in Somalia and, in more recent times, the Boko Haram sect in Nigeria, the ISIS and ISIL in Iraq, Syria, Egypt and Libya, and the Al-Mourabitoun terrorist group in Mali.

Over the years, the various terrorist groups have become so powerful that governments are finding it increasingly difficult to curtail their activities. Many of the terrorist groups acquire more sophisticated weapons than many countries' security agents. In some cases also, they operate in networks across sovereign nations and this makes them more

formidable and elusive to many governments' control. In this age of information revolution, more than ever before, it is much easier for terrorists residing in different parts of the world to collaborate and jointly plan attacks and bombings. Hence, intelligence gathering is currently more beneficial and effective in combating terrorism than the conventional means of fighting crimes.

Terrorists make use of the Information and Communication Technology (ICT) to plan and execute their attacks. Hence, it has become imperative for governments to employ the same tool in their attempt to combat terrorism which has become a great impediment to the quest for development and sustainable social order in many parts of the world, especially in Africa.

Spyware, Surveillance, Electronic Espionage and Intelligence Gathering

Spyware refers to 'a program placed on a computer without the user's knowledge that secretly collects information about the user. … The spyware program communicates information it collects to some outside source while you are online' (Shelly and Vermaat 2008, 381). Spyware is a programme which an internet user unwittingly installs on her computer because it usually comes as a hidden component of freeware, shareware and commercial software programmes, which one could easily download from the internet. Once installed, it secretly collects personal information about the user and sends it to the author or the web base of the spyware. Spyware gathers useful personal information like account details, passwords, credit card numbers, phone numbers, medical condition of the infected host and e-mail addresses. Information gathered by a spyware can be used for different purposes, depending on the intent of the author of the software. According to Newman, 'intelligence gathered can be relayed to the spyware author, who will either use it for advertising/marketing purposes or sell the information to another party' (Newman 2010, 52).

Sometimes, spyware comes from phishers who employ botnets and e-bait to lure people into giving out information about themselves, their business or their health. According to Baskin et al,

> Hackers can use both botnets and phishing attacks to deliver spyware to a host. In the phishing attack, the hacker sends the "bait" in the form of e-mail requiring urgent attention to avoid unpleasant consequences. The e-mail tells the user to click on a link that appears to take them to a Web site that they trust. At this Web site, the hacker can gather account information and/or passwords or can upload a Trojan (most likely a remote access Trojan) for these purposes (Baskin et al 2006, 88).

Certain features are basic to an efficient spyware programme. The features include the ability of a spyware programme to hide, collect, communicate and survive. In other words, an effective spyware must be able 'to operate in the background, collect information, communicate this information to a third party, and maintain a presence in a computer system. In short: hide, collect, communicate and survive in a hostile environment' (Barwinski, Irvine and Tim 2006, 2). Although, spyware has mostly been used for hacking and advertisement purposes, in this age of high terrorist insurgencies, which are mostly planned with the help of Information Technology, the use of spyware to gather security information on planned terrorist attacks is not out of place. In other words, because of the advanced technical know-how involved in the planning of terrorist attacks in contemporary times, it has become imperative for security agencies to employ methods beyond the traditional means of controlling crimes in dealing with the menace of terrorism. In an attempt to combat terrorism and modern-day crimes, security agencies have found intelligence gathering to be very invaluable. One of the current tools of intelligence gathering that could prove useful, however, is spyware.

Intelligence gathering involves gathering information about a particular crime, terrorist act or terrorist group before any step is taken to stop such criminal or terrorist act. As a matter of fact, 'effective intelligence-gathering, threat analysis and dissemination is the first line of defence against terrorism' (Kelly and Hays 1987, 60). In contemporary militarism, the

importance of intelligence gathering cannot be overemphasized. Intelligence gathering is not a recent tactic in warfare. In the earliest centuries of warfare, history reveals that people had consulted the spirits and deities to know the outcome of battles before they embarked on such battles. However, Dulles (2006) relates that people were sometimes defeated in spite of waging wars based on the findings from such consultations. The reason for this, according to him, is that knowledge gotten from such spiritual sources is most times shrouded in mystery and ambiguities. Therefore, Dulles also agrees with an ancient Chinese sage that intelligence gathering about the enemy ensures victory. According to Dulles,

> But in the craft of intelligence, the East was ahead of the West in 400 B.C. rejecting the oracles and the seers, who may well have played an important role in still earlier epochs of Chinese history, Sun Tzu takes a more practical view. 'What is called "foreknowledge" cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations', he wrote. 'It must be obtained from men who know the enemy situation' (Dulles 2006, 4).

As a matter of fact, humans and animals have been employed for the purpose of espionage both in war and peace times over the years. In fact, apart from humans, one animal that has been found useful in espionage is dogs. 'The East German police, army, and the Stasi had their share of border and guard dogs trained for espionage and security purposes, in which the dog's nose, not its bark, played a central role' (Macrakis 2008, 283). However, electronic and technical espionage has been observed to be more effective and less risky that human and animal intelligence gathering. According to Macrakis, 'using human sources had high risks: agents get captured and jailed; officers defect and spill the beans. By contrast, technical intelligence has fewer dangers (Macrakis 2008, 254).

Meanwhile, with the herald of the digital age, human espionage or intelligence gathering using animals and humans is no longer as efficient as before the World War II. This is because apart from the fact that losses incurred could be great in cases where humans are caught spying – this, for example, could lead to loss of lives – this method is also no longer effective because enemies, especially terrorists working together, are no longer restricted to

any particular geographical location. This, therefore, makes it imperative that electronic espionage and surveillance be employed to combat terrorism in these contemporary times.

Traditionally, spyware, espionage and electronic surveillance are used for different purposes. For instance, spyware is used by hackers to get information about people, which could be used to get to them buy certain products and services and it is mostly regarded as a cybercrime in many countries. Espionage and intelligence gathering are, in most cases, tools employed by countries at war to monitor each other, especially to discover each other's vulnerable points. However, for surveillance, this apparatus is used by the state in some countries to monitor the activities of their citizens, although whether this is morally right is a different question altogether. Hackers have been using spyware mainly for economic purpose for a long time. The use of spyware has, however, in recent times assumed a political dimension. In other words,

> Organized crime and unscrupulous marketing companies have generated lucrative market for hacking4hire, clicks4hire, and other schemes for generating revenue through hacking skills. These schemes have included ransomware (holding a website or personal information hostage in exchange for cash) theft of financial account information, identity theft, storage of illegal files (e. g., child porn, stolen Intellectual Property, cyber vendettas), and theft of encryption keys. To this list, governments and global corporation have added intelligence gathering, economic or industrial espionage and information warfare (Baskin et al 2006, 131).

Therefore, it has been alleged that spyware is being employed by some government security agencies for surveillance purposes. In cases whereby certain persons are suspected of being involved in one criminal activity or the other, spyware is believed to be one effective means of secretly spying on such people's activities on the internet for the purpose of gathering useful information about them either to forestall a crime that is being planned or to nab them for a crime already committed. Although, it is difficult to establish the fact of governments or their agencies using spyware, this is, however, not outright impossible. This is because, 'evidence of government spyware is difficult to find, but a couple of espionage cases involving software have been attributed to governments' (Baskin et al 2006, 86). As a

matter of fact, some tiny pieces of evidence filter out from time to time to strongly suggest that governments actually resort to the use of spyware or hacking of information for espionage, surveillance or intelligence gathering. For example,

> In November 2001, MSNBC reported that the FBI was developing a technology called Magic Lantern, which was essentially a Trojan horse that installed keystroke logger on a suspect's computer. The FBI used similar software to gain encryption codes via keylogging the computer of Nicodemo Scarfo, a member of the Gambino crime family (Baskin et al 2006, 87).

Perhaps when it comes to fighting terrorism, the line between crime and war gradually fades. In some cases, because terrorists combine methods employed by domestic criminals and those used by external aggressors to wage wars, it may become imperative for security agencies to also develop a strategy that sees terrorism as both a war and a crime and addresses it as such. However, the extent to which a government can go in addressing the menace of terrorism as both crime and war becomes questionable in a democracy, especially in a liberal democracy.

Liberal Democracy and Rights of the Individual

The required extent of involvement of the state in regulating the individual has remained one of the core concerns of political philosophers of all ages. In other words, political philosophers have variously sought for ways to reconcile the ideas of corporate existence and individual existence or put differently, the 'moralities of communal ties and the moralities of individuality' (Chisick 2000, 101). Modern political philosophers, especially the social contract theorists, namely, Hobbes and Rousseau, for example, proposed that when the existence of the individual seems to be at loggerheads with corporate existence, the state apparatuses should be employed to subject the individual to the exigencies of corporate existence. Justification for this is believed to lie in the consent which the individual freely gives at the point of enacting the social contract. Even Rousseau, who seems to recognise that authority resides with the people, holds that the rights of the individual is believed to be

subsumed under the general will such that the individuality of the individual disappears in the grim view of corporate existence. However, liberal democracy, which has its basis in the political idea of John Locke, holds that the individual is the basis of governance. This is because the 'liberalism embodied in liberal democracy is linked both to the constitutional heritage of the rule of law and parliamentary institutions, and to a democratic belief in the acceptance of the majority will' (Carter 2010, 118). These two ideas can be found in Locke's social contract idea. The rights of the individual find much expression in liberal democracy.

The merger of the idea(l)s of liberalism and democracy emphasises the centrality of the individual, especially the centrality of the rights and freedom of the individual to governance. This is because democracy implies the consent of the governed, which consent rests, explicitly or implicitly, on the recognition of the effective political equality of the individuals who constitute the *demos*. Liberalism, however, implies a respect for the individual qua individual (Watson 1999, 3).

Concepts like equality of persons, freedom and liberty of individuals form the basis of every true liberal democracy. As a matter of fact, if the concepts are not present in any system of government, such a system of government cannot be described as a liberal democratic form of government. The reason for this is that,

> The liberty of the individual is an essential and fundamental element of every genuine *liberal democracy*, including a variety of democracies that emphasise consensus and solidarity of the political community. In the absence of the liberty advocated by liberalism, the individual may be subjugated in the name of the community or other values (Center for Civic Education 2007, 50).

In recent years, liberal democracy has attained recognition in most parts of the world as the most ideal form of government. This recognition stems from two important sources. In the first place, the failure of communism in Russia and China makes it seem evident that liberal democracy, which has lasted for centuries in the United States of America is a better and more plausible alternative. On the other hand, liberal democracy has been seen to have

worked for centuries in America and with the power that the United States wields in the comity of nations, it becomes easy to sell the idea of liberal democracy to the rest of the world. According to Fukuyama, history has revealed that liberal democracy, founded on the twin principles of equality and liberty, has successfully 'conquered rival ideologies like hereditary monarchy, fascism, and most recently communism' (Fukuyama 2006, xi). Fukuyama further states in relation to the triumph of liberal democracy as a system of government that, "While some present-day countries might fail to achieve stable liberal democracy, and others might lapse back into other, more primitive forms of rule like theocracy or military dictatorship, the *ideal* of liberal democracy could not be improved on" (Fukuyama 2006, xi).

Fukuyama ties the triumph of liberal democracy over rival ideologies about governance to legitimacy. For him, liberal democracy is a legitimate form of government, while those other ideologies essentially lack the element of legitimacy. The element of legitimacy accounts for the perennial relevance of liberal democracy as a system of government. In his words,

> Authoritarian regimes on the Right and Left … have sought to use the power of the state to encroach on the private sphere and to control it for various purposes – whether to build military strength, to promote an egalitarian social order, or to bring about rapid economic growth. What was lost in the realm of individual liberty was to be regained at the level of national purpose. The critical weakness that eventually toppled these strong states was in the last analysis a failure of legitimacy – that is, a crisis on the level of ideas. … All regimes capable of effective action must be based on some principle of legitimacy (Fukuyama 2006, 15).

Fukuyama, owing to the alleged indisputable triumph of liberal democracy, recommends it as a universally valid system of government. At the end of the twentieth century, Fukuyama boldly declared that:

> As mankind approaches the end of the millennium, the twin crises of authoritarianism and socialist central planning have left only one competitor standing in the ring as an ideology of potentially universal validity: liberal democracy, the doctrine of individual freedom and popular sovereignty. Two hundred years after they first

> animated The French and American revolutions, the principles of liberty and equality have proven not just durable but resurgent (Fukuyama 2006, 42).

However, there exists no doubt a tension between enhancing the individuality of individuals as emphasised by liberalism and safeguarding the common good which is fundamental to democracies. The tension, in other words, exists between 'the *ideas* that ground and would preserve liberal democracy, on the one hand, and the ideas that are at the core of self-expressive, and possessive, individualism, on the other' (Watson 1999, 4).

Terrorism and Security Threats in Contemporary Times

Ever since terrorists attacked the World Trade Centre in New York in 2001, terrorism has attracted the attention of the world as a menace of global concern. The reason being that apart from the fact that the WTC is a significant symbol of Western capitalist economy, the magnitude of the attack was also such that it could not but raise fundamental questions about global security and safety. Giving succinct descriptions of the impact of the September 11 terrorist attack, Burke and Cooper note that:

> Almost 2800 lives were lost and this was the worst terrorist attack in US history … the events of 9/11 have changed many parts of the world forever. The events of 9/11 were unique. The number of deaths was unprecedented, and includes those of 343 firefighters who lost their lives responding to the attacks. The terrorists did not need weapons of mass destruction to cause mass casualties and more than $90 billion in losses. The airline, insurance and tourism industries were particularly hard hit (Burke and Cooper 2008, x).

Another point of worry is that Al-Qaeda which was responsible for the massive attacks of September 11 has since metamorphosed into an array of other powerful and equally deadly, or even deadlier, groups since 2001. For example, in addition to Al-Qaeda, other terrorist groups that have sprung up include Jemaah Islamiyah and the Abu Sayyaf Group in Southeast Asia, Islamic Army of the Abayan Aden, the Islamic Combatant Group, and Salafi Group for Call and Combat in Algeria (Richardson 2004, vii-viii). These groups unleash a frightening magnitude of terror on different nations of the world.

The question is why would someone unleash terror on people who they have never met before, has not offended or wronged them or whose faces they do not even know? These questions are very important to consider in relation to recent numerous cases of indiscriminate terror attacks because, 'terrorist attacks are not aimed at members of an army in conditions of combat. Rather, they target ordinary people riding on a bus, shopping in a market, or going to work. Why is this?' (Nathanson 2010, 28). Different answers reasons have been suggested regarding why some people would just wake up and launch deadly attacks on unsuspecting innocent people and get themselves and scores (even thousands) of other people killed or injured. An answer to this question has it that the main aim of terrorists is to frighten people or instil fear in people's hearts. It is held that terrorists create fear, in most cases, to register their displeasure, grievances or frustrations against a particular government or society. Therefore, they usually do not mind who gets hit, killed or maimed as long as they are able to get the message across to the appropriate quarters.

Another explanation is that terrorists are in some cases attention seekers who are trying to get noticed or just merely want to be popular since terrorist activities enjoy a great deal of publicity in the media. By and large, however, whatever reason is given for a terrorist attack, either plausible or not, and whether it exonerates or implicates the terrorists, a significant part of the responsibilities of a government either a liberal democracy or any other form of government, is to ensure that its citizens are safe. This is because, "While we expect soldiers to be attacked in war, we do not expect civilians – people who are typically not engaged in fighting and who are going about the ordinary activities of daily life – to be attacked for political purposes. This is what makes terrorist attacks so shocking" (Nathanson 2010, 29).

Terrorism is not so to speak a recent phenomenon. But "while terrorism is a phenomenon that is continuously reinventing itself, the lack of continuity between each

generation of terrorists often entails a signal break with the past" (Chaliand and Blin 2007, 6, it is not). In spite of the 'break with the past', however, it is noteworthy that each generation of terrorists makes use of the means or inventions available in their generation which are believed to be capable of better enhancing their terrorist activities.

Therefore, it is rather not surprising then that in this age of information revolution, terrorists also employ inventions and innovations in ICT both in the planning and execution of terrorist acts. In fact for terrorists, at this age of information revolution, mounting an attack might not be possible at all without the use of technology in one form or another. For example, Al-Qaeda is known to have used computers to help plan and prepare attacks as early as 1993. According to the National Commission on Terrorist Attacks, upon the United States, both the 1993 and 2001 attacks on the World Trade Center made use of computers in various ways, from managing communications to helping plan the attacks in depth (Bocij 2006, 6).

Apart from just using computers, it has recently become extremely difficult in recent years to carry out any activities that involve planning without the use of information technology or the internet in particular. Terrorist attacks require careful planning and the role of ICT cannot be overemphasised. This makes it obvious that if terrorist activities are to be discovered and forestalled, the importance of ICT cannot be undermined. This is because,

Terrorists use cyberspace as a tool, and leave "footprints" in cyberspace: "This low-intensity/low-density form of warfare has an information signature, albeit not one that our intelligence infrastructure and other government agencies are optimized to detect. In all cases, terrorists have left detectable clues that are generally found after an attack." These clues include data on operational planning and execution, specific acts of surveillance and reconnaissance, transactions, practice runs, and increases in communications (e.g. "chatter") (Pollard 2006, 239).

Government and security agencies can get a lot of clues that would enable them to uncover and forestall terrorist attacks and thereby enhance the safety of their citizens. For instance, 'these clues indicate what terrorists are planning, what they are targeting, how they communicate and provide resources, and even how their networks are formed. These clues exist especially for those activities that terrorists have always conducted before an attack (Pollard 2006, 239).

Therefore, data mining that spyware makes available could serve as a means of detecting terrorist activities from recruitment to radicalisation, training and actual planning of a particular attack. This, however, raises serious questions about not interfering in ordinary citizens' private lives. In other words, is sacrificing one's privacy a just price for safety? Also, at what point of security threat are government agencies justified to intrude into people's privacy? Can we find any basis of justification for intruding into the privacy of other members of society when there is a serious security challenge in the nation?

A Utilitarian Approach to Ethical Judgments

Utilitarianism is a traditional ethical theory which has struck the necessary balance between the self-regarding egoism and the other-regarding but self-disregarding altruism. Utilitarianism holds an approach to ethical thinking which claims that 'the rightness or wrongness of any action is dependent entirely on the outcomes that derive from it. In other words, neither the intent behind the action nor the fundamental rightness or wrongness of the action is at issue, only the consequences' (Parsons 2005, 44). Therefore, what matters most in a utilitarian consideration of what is ethical is the consequence or the likely or potential outcome of an action. This makes utilitarianism a teleological ethical theory. This is because, according to teleological theory (also known as consequentialism), actions can only be judged right and/or good on the basis of the consequences they produce (Johnstone 2009, 64). This is a general claim for teleological or consquentialist theories. To be specific, however,

utilitarianism avers that the right action is the one that, out of all the available alternatives, creates the greatest balance of happiness over unhappiness (Bennett 2015, 55). In other words, utilitarianism has,

> As its central concern the general welfare of people as a whole, rather than individuals ... utilitarianism views the world not in terms of certain individual rights which people may or may not claim, but in terms of people's collective and overall welfare and interests. The perspective of utilitarianism ... promotes a universal point of view; namely, that one person's interests cannot count as being superior to the interests of another. ... I cannot claim (for example) that my interests are more deserving than your interests are, just because they are my interests (Johnstone 2009, 64).

Utilitarianism, therefore, holds that what makes an action morally right or wrong must put the total number of people affected by the action into consideration. In other words, the utilitarian maxim advocates that the morality of a decision be based on the number of people affected, so that the moral consideration can serve the public good by benefitting the majority (Bowen 2005, 79). For utilitarianism, it is the welfare of the greater number that matters. Hence, utilitarianism adopts the ethical stance of seeing every individual in any particular society as counting for one and not more than one. Therefore, it does not matter whether someone is a monarch or a pauper, utilitarianism views such an individual as just one person whose comfort or pain can have a contributory effect to the status of corporate morality and corporate existence, while it cannot solely determine the course of corporate morality.

On the issue of utilitarianism versus individual's autonomy to exercise her right, it could be argued that there are also serious persuasive utilitarian reasons why people's rights to their privacy should be considered of more fundamental importance which must not be violated. It can be raised, for example that why should the government bring discomfort to a number much greater than the few terrorists which they are seeking to nab. Hence, it can be contended that pain is brought to the much greater number than the number of the people targeted.

In this case, it is important to allude to the hedonistic calculus which shows that pleasures and pains are of varying degrees and this determines the extent to which they can justify a particular action. The hedonistic calculus need not be a mathematical calculation. With reason and commonsense, however, it is meant to guide us to choose a more plausible and pragmatic course of action. In other words,

> Bentham's hedonistic calculus, with its seven dimensions of pleasure and pain, intensity, duration, probability, proximity, fecundity, purity and extent, was never presented as something which could be used in any mechanical or precise way. Rather it specified an ideal ground for decision making, not fully available to us in practice, to which our grounds of decision making should approximate so far as possible (Sprigge 2000, 134).

Evaluating and juxtaposing data-mining and surveillance in the form of spyware and the right to privacy by the hedonistic calculus shows that what brings safety to the greater number becomes more important as an ethical standard. In this sense,

Pleasures and pains can thus be weighed, ranked and traded off – and the putative symmetry of the continuum will guarantee a rational-choice outcome. This alleged symmetry not only endowed the hedonistic calculus with perfect rationality, it also provided a basis for interpersonal (and thus objective or inter subjective) standards by which the claims of competing individuals might be adjudicated (Barber 2003, 84).

Conclusion

Dilemmas are a very familiar part of ethical judgments. in real life everyday cases as in hypothetical ethical conjectures, individuals come across insoluble conflicts between equally compelling but directly competing moral requirements, and thus have to violate or fail to satisfy at least one of them (Davis 2005, 487). Therefore, in a situation whereby individuals and even corporate or political bodies are faced with moral dilemmas, it is imperative to determine whether the two moral requirements are actually equally weighty.

In the case of the dilemmas involved in the moral requirements of ensuring that people's privacy is respected versus the one of ensuring people's safety at all costs even if it means

that the meddling tool of spyware is employed at least for the purpose of surveillance, utilitarianism is considered very instructive in addressing the quandary. In light of the position of utilitarians,

> Utilitarianism's basic idea is that what makes actions morally right and wrong is their impact on the well-being of human beings. According to "act utilitarianism," the theory's most familiar and most radical form, any action is right if it produces better consequences in a particular situation than any alternative actions produce. Reacting against both custom and taboo moralities that judge the morality of actions independently of their effects, utilitarianism tells us to look to the consequences of actions. Nothing else matters (Nathanson 2010, 88).

In other words, utilitarianism as an ethical standard is particular about the nature of the consequences that actions produce in the bid to determine whether such actions are morally right or wrong. The fundamental question then is whether non-interference with people's privacy promotes well-being of humans the exact way surveillance does. As a matter of fact, humans forget their rights to privacy in the face of life-threatening dangers. When people are in dire need of rescue, say, in the case of a disaster, they do not claim a private life that other people cannot pry into. Occasional occurrences of disasters, be it man made, like terrorism, or natural disasters, emphasise and make obvious our mutual vulnerability and indispensability of interconnectedness to our survival as humans. Therefore, an excessive claim to privacy, as advocated by liberal democracy which overlooks the important facts of our vulnerability as humans is a theory that stands survival on its head.

This is not an attempt to advocate that government agencies should meddle in people's private affairs at will, it is however an attempt to underscore the idea that when survival is at stake, especially as made obvious by security threats posed by recent terrorist challenges, reason demands that privacy take the second place in the scheme of priorities.

References

Barber, Benjamin R. 2003. *Strong Democracy: Participatory Politics for a New Age.* Berkeley: University of California Press.

Barwinski, Mark, Cynthia Irvine and Tim Levin. 2006. "Empirical Study of Drive-by-Download Spyware." In *Proceedings of the International Conference on i-Warfare and Security 2006: ICIW 2006*, Leigh Armistead, 1-15. England: Academic Conferences and Publishing.

Baskin, Brian, Tony Bradley, Jeremy Faircloth, Craig A Schiller, Ken Caruso, Paul Piccard and Lance James. 2006. *Combating Spyware in the Enterprise: Discover, Detect and Eradicate the Internet Greatest Threat.* Massachusetts: Syngress Publishing.

Bennett, Christopher. 2015. *What is this Thing Called Ethics?* London: Routledge.

Bocij, Paul. 2006. *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals.* Westport, Connecticut: Praeger.

Bowen, Shannon A. 2005. "Communication Ethics in the Wake of Terrorism." In *Community Preparedness and Response to Terrorism: Communication and the Media,* eds.

Dan H. O'Hair, Robert L. Heath, and Gerard Ledlow, 65-96. Westport, Connecticut: Praeger.

Burke, Ronald J and Cary L. Cooper. 2008. *International Terrorism and Threats to Security: Managerial and Organizational Challenges.* Massachusetts: Edward Elgar Publishing.

Carter, April. 2010. *Direct Action and Liberal Democracy.* Oxon: Routledge.
Center for Civic Education. 2007. *Elements of Democracy: The Fundamental Principles, Concepts, Social Foundations and Processes of Democracy,* California: Center for Civic Education.

Chailand, Gerard and Arnaud Blin. 2007. *The History of Terrorism: From Antiquity to Al Qaeda.* Berkeley: University of California Press.

Chan, Sylvia. 2002. *Liberalism, Democracy and Development.* Cambridge: Cambridge University Press.

Chisick, Harvey. 2000. "The Dual Threat to Modern Citizenship: Liberal Indifference and Nonconsensual Violence." In *Liberal Democracy and the Limits of Tolerance: Essays in Honor and Memory of Yitzhak Rabin*, ed. Raphael Cohen-Almagor, 99-113. Ann Arbor: The University of Michigan Press.

Davis, Ann N. 2005. "Moral Dilemmas." In *A Companion to Applied Ethics*, ed. R. G. Frey and Christopher Heath Wellman, 487-497. Maiden: Blackwell Publishing.

Dulles, Allen W. 2006. *The Craft of Intelligence: America's Legendary Spy Master: On the Fundamentals of Intelligence Gathering for a free World*. Connecticut: The Lyons Press.

Espeseth, Craig, Gibson Jessica, Andy Jones and Seymour Goodman. 2013. "Terrorist Use of Communication Technology and Social Networks." In *Technological Dimensions of Defence against Terrorism,* ed. Feyyaz U. Aydogdu, 91-105. Amsterdam: IOS Press.

Fukuyama, Francis. 2006. *The End of History and the Last Man.* New York: Free Press.

Johnstone, Megan-Jane. 2009. *Bioethics: A Nursing Perspective.* Sydney: Elsevier.

Kelly, William M. and Daniel P Hays. 1987. *The Report of the Senate Special Committee on Terrorism and the Public Safety.* Darby: Diane Publishing Company.

Nathanson, Stephen. 2010. *Terrorism and the Ethics of War.* Cambridge: Cambridge University Press.

Newman, Robert C. 2010. *Computer Security: Protecting Digital Resources.* London: Jones and Bartlett Publishers.

Parsons, Patricia J. 2005. *Ethics in Public Relations: A Guide to Best Practice.* London: Kogan Page.

Pollard, Neal. 2006. "Counter-terrorism in Cyberspace: Opportunities and Hurdles." In *Countering Terrorism and WMD: Creating a Global Counter-terrorism Network,* ed. Peter Katona, Michael D. Intriligator and John P. Sullivan, 235-252. London: Routledge.

Richardson, Michael. 2004. *A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction.* Singapore: Institute of Southeast Asian Studies Publications.

Shelly, Gary B. and Misty E Vermaat. 2008. *Discovering Computers: Fundamentals.* New Boston: Cengage Learning.

Sprigge, T. L. S. 2000. "Is the Esse of Intrinsic Value Percipi?" In *Philosophy, the Good, the True and the Beautiful,* ed. Anthony O'Hear. Cambridge: Cambridge University Press.

Watson, Bradley C. S. 1999. *Civil Rights and the Paradox of Liberal Democracy.* Lanham: Lexington Books.